On independent sets of elements in algebra*)

By A. KERTÉSZ in Debrecen

To Professor L. Rédei on his 60th birthday

§ 1. Introduction

In connection with the different concepts of "independence" which arise in the investigation of different algebraic structures, there are known theorems which assert that maximal independent sets of elements must have the same cardinality. Making use of what is really a generalization of the essence of STEINITZ's exchange theorem, we give in the present note a method which can advantageously be employed in proving theorems of this type (Theorem 1). Some applications of Theorem 1 are found in § 3. There in particular we determine the class of all those associative rings R for which any two maximal independent systems of elements of any torsion free R-module have the same cardinal number.

§ 2. Abstract dependence

Let S be an arbitrary set and $D[x, A]$ a binary relation defined between elements x and subsets A of S, satisfying the following conditions:

(I) If $x \in A$, then $D[x, A]$.

(II) If $D[x, A], a \in A$ and $\bar{D}[x, A \setminus \{a\}]$, then $D[a, (A \setminus \{a\}) \cup \{x\}]$.[1])

(III) If $D[x, A]$ and $D[a, B]$ for all elements $a \in A$, then $D[x, B]$.

(IV) If $D[x, A]$, then there exists a finite subset A' of A such that $D[x, A']$.

If $D[x, A]$ holds, we say that x *depends on* A. We say that *the set* $A (\subseteq S)$, *depends on the set* $B (\subseteq S)$, if each element of A depends on B,

*) This paper was presented at a scientific session at Debrecen University in April 1959.

1) By $\bar{D}[x, B]$ we denote the fact that the relation $D[x, B]$ is not valid. In the case of two sets A and B, $A \setminus B$ denotes the set of those elements of A which are not contained in B. The empty set is denoted by $\emptyset$, and the cardinal number of A is $|A|$.

and in this case we write $D[A, B]$. If $D[A, B]$ and $D[B, A]$ both hold, then A and B are said to be *D-equivalent.* A set $A(\subseteq S)$ is said to be *D-dependent,* if there exists an element a in A such that $D[a, A\setminus\{a\}]$. In the contrary case A is said to be *D-independent.* On the basis of (IV) it is clear that a set A is D-independent if and only if each of its finite subsets is D-independent.

If we suppose that in the relation $D[x, A]$ the set A is always finite, then the properties (I′), (II′), (III′) corresponding in this special case to (I), (II) and (III) are exactly the well known axioms of abstract dependence. It is also known that (I′), (II′) and (III′) imply that *two finite independent equivalent sets have the same number of elements.*[2]) With the aid of (I)—(IV) we are now going to prove this theorem in the general case. It is possible to give a proof which reduces the problem to the finite case;[3]) we give here, however, a direct proof in which the finite case plays no distinguished role.

Theorem 1. *Let $D[x, A]$ be a relation defined on a set S and satisfying the conditions* (I)—(IV). *Then any two D-equivalent D-independent subsets of S have the same cardinal number.*[4])

Proof. Let $H(\subseteq S)$ and $K(\subseteq S)$ be two D-equivalent D-independent sets. Owing to symmetry it will be sufficient to show that if $|H| = \mathfrak{m}$, then $|K| \geqq \mathfrak{m}$.

Let the symbol

$$(H', K', \varphi') \tag{1}$$

express the fact that φ' is a one-to-one mapping of the set $H'(\subseteq H)$ onto the set $K'(\subseteq K)$, and that the set $R' = K' \cup (H\setminus H')$ is D-independent. We denote by Q the set of all triplets (1). This set is certainly non-empty, since we allow also the possibility of H', K' being empty sets and φ' the empty mapping. Q can be turned into a partially ordered set by agreeing that for two different triplets (H', K', φ') and (H'', K'', φ'')[5]) the relation $(H', K', \varphi') < < (H'', K'', \varphi'')$ holds if and only if $H' \subset H''$, $K' \subset K''$ and φ'' is a continuation of φ'. We show that the set Q is inductive, i. e. each ordered subset

$$\cdots < (H', K', \varphi') < (H'', K'', \varphi'') < \cdots \tag{2}$$

---

[2]) See e. g. van der Waerden [11], § 36, and Pickert [8].

[3]) In this connection we refer to the method employed in [5].

[4]) The author had access to a paper by M. N. Bleicher and G. B. Preston on "Abstract linear dependence relations" awaiting publication in *Publicationes Mathematicae Debrecen.* This theorem is also proved there, but on quite different lines.

[5]) Two triplets (H', K', φ'), (H'', K'', φ'') are to be considered different if at least one of the relations $H' \neq H''$, $K' \neq K''$ and $\varphi' \neq \varphi''$ holds.

of Q has an upper bound in Q. We indeed have

$$\cdots \subset H' \subset H'' \subset \cdots; \quad \cdots \subset K' \subset K'' \subset \cdots.$$

Let us consider the subsets

$$H_0 = \cdots \cup H' \cup H'' \cup \cdots \ (\subseteq H) \qquad \text{and} \qquad K_0 = \cdots \cup K' \cup K'' \cup \cdots \ (\subseteq K).$$

First we remark that $R_0 = K_0 \cup (H \setminus H_0)$ is D-independent, since any finite subset of R_0 is contained in a suitable set of the form $R' = K' \cup (H \setminus H')$, and such a set is D-independent. Moreover it is clear that there exists a one to one mapping φ_0 of H_0 onto K_0 which is a continuation of each of the mappings φ in (2). So (H_0, K_0, φ_0) is an upper bound of (2).

Thus by the lemma of KURATOWSKI—ZORN Q has a maximal element (H^*, K^*, φ^*). We show that $H = H^*$. If this is true, then $R^* = K^* \cup (H \setminus H^*) = K^* \subseteq K$; in view of the equal cardinality of H^* and K^* the set R^* has cardinality $\mathfrak{m}$, so that $|K| \geqq \mathfrak{m}$.

Suppose our assertion to be false, i.e. $H^* \subset H$. First note that in this case H has an element h which is also an element of R^*, and K has an element k for which $\overline{D}[k, R^* \setminus \{h\}]$ holds and so, by (1), $k \notin K^*$. For if we had $D[K, R^* \setminus \{h\}]$, then by $D[h, K]$ and (III) the relation $D[h, R^* \setminus \{h\}]$ would also hold, contradicting the D-independence of R^*. Secondly, the set $R^{**} = (R^* \setminus \{h\}) \cup \{k\}$ is D-independent. Otherwise there would exist an element $r (\in R^{**})$ for which $D[r, R^{**} \setminus \{r\}]$: if $r = k$, then we have at once $D[k, R^* \setminus \{h\}]$, a contradiction; if $r \neq k$, then with the help of $\overline{D}[r, R^{**} \setminus \{r, k\}]$ and (II) we again have $D[k, R^* \setminus \{h\}]$. Finally denoting by φ^{**} the mapping of $H^* \cup \{h\}$ onto $K^* \cup \{k\}$ which arises if we complete the mapping φ^* of H^* onto K^* by the mapping $h \to k$, we get

$$(H^*, K^*, \varphi^*) < (H^* \cup \{h\}, K^* \cup \{k\}, \varphi^{**}),$$

which contradicts the maximality of (H^*, K^*, φ^*). This completes the proof of Theorem 1.

We remark that since by (IV) the D-independence defined above is a property of finite character, according to the lemma of TEICHMÜLLER—TUKEY the set S has a maximal D-independent subset. It is also clear that two maximal D-independent subsets are equivalent, and this gives us the following corollary to our theorem:

Corollary. *Any two maximal D-independent subsets of the set S have the same cardinality.*

§ 3. Applications

1. Let M be an arbitrary set. Following WHITNEY [12], we define a *rank function* r on M which associates with every finite subset A of M a non-negative integer $r(A)$ satisfying the axioms (R_1), (R_2), (R_3) as follows:

(R_1) $r(\emptyset)=0$,

(R_2) $r(A\cup\{x\})=r(A)+k$, where $k=0$ or 1,

(R_3) if $r(A)=r(A\cup\{x\})=r(A\cup\{y\})$ then $r(A)=r(A\cup\{x,y\})$.

A finite set $A(\subseteq M)$ is said to be *r-independent* if $r(A)=|A|$. We say that the arbitrary set $A(\subseteq M)$ is r-independent if each of its finite subsets is r-independent.

As a first application of Theorem 1 we prove the following theorem of R. RADO [9]:

Any two maximal r-independent subsets of the set M have the same cardinality.

Let us be given on the set M the function $r(A)$. We define on M a relation $D[x,A]$ in the following way: $D[x,A]$ is to be valid if and only if there exists a finite subset A' of A such that $r(A'\cup\{x\})=r(A')$. In view of the evident fact that on M the concepts of r-independence and D-independence coincide, in order to prove the theorem of RADO with the aid of the Corollary of Theorem 1, it will be sufficient to show that for the relation $D[x,A]$ conditions (I)—(IV) are satisfied.

It is clear that (I) and (IV) hold. Suppose now $D[x,A]$, $a\in A$ and $\overline{D}[x,A\setminus\{a\}]$ to be valid. Then A has a finite subset A' for which

$$r(A')=r(A'\cup\{x\}), \tag{3}$$

$$r(A'\setminus\{a\})<r((A'\setminus\{a\})\cup\{x\}) \tag{4}$$

hold. On the basis of (R_2) we obtain from (4) with the aid of (3)

$$r(A')\leqq r((A'\setminus\{a\})\cup\{x\})\leqq r(A'\cup\{x\})=r(A')$$

and consequently

$$r((A'\setminus\{a\})\cup\{x\})=r(A'\cup\{x\})$$

which shows $D[a,(A'\setminus\{a\})\cup\{x\}]$ to be true, proving so the validity of (II).

In order to show that (III) is also valid, we shall need two simple lemmas:

Lemma 1. *If* $r(A)=r(A\cup\{x_1\})=\cdots=r(A\cup\{x_n\})$, *then* $r(A)=$ $=r(A\cup\{x_1,\ldots,x_n\})$.

Our assertion is true for $n=2$ by (R_3). We suppose it to be valid for $n-1$. Then $r(A)=r(A\cup\{x_1,\ldots,x_{n-2},x_{n-1}\})=r(A\cup\{x_1,\ldots,x_{n-2},x_n\})$. Making use again of (R_3) we get $r(A)=r(A\cup\{x_1,\ldots,x_n\})$.

L e m m a 2. *If* $r(A)=r(A\cup\{x\})$, *then for any finite set* Y *the relation* $r(A\cup Y)=r(A\cup Y\cup\{x\})$ *holds.*

It will clearly be sufficient to prove our assertion for the case $Y=\{y\}$. If $r(A\cup\{y\})=r(A)$, then $r(A)=r(A\cup\{x\})$ and by (R_3) $r(A\cup\{y\})=r(A\cup\{x,y\})$. On the other hand if $r(A\cup\{y\})=r(A)+1$, then by $r(A\cup\{x,y\})\geqq r(A\cup\{y\})\geqq \geqq r(A)=r(A\cup\{x\})$ and by (R_2) $r(A\cup\{x,y\})=r(A)+1$, i. e. $r(A\cup\{y\})= =r(A\cup\{x,y\})$ also holds.

Suppose now $D[x,A]$ and $D[a,B]$ to be valid for any element $a\in A$. We show that in this case $D[x,B]$ also holds. Without prejudice to generality we may suppose that $A=\{a_1,\dots,a_n\}$ and B are finite. Since by our hypotheses and Lemma 2 $r(A)=r(B\cup a_i)$ for $i=1,\dots,n$, in view of Lemma 1 we get

$$r(B)=r(A\cup B). \tag{5}$$

On the other hand, by virtue of $r(B\cup\{a_1\})=r(B)$ and of Lemma 2 we obtain

$$r(B\cup\{a_1,x\})=r(B\cup\{x\}), \tag{6}$$

and by virtue of $r(B\cup\{a_2\})=r(B)$ and of Lemma 2

$$r(B\cup\{a_1,a_2,x\})=r(B\cup\{a_1,x\}). \tag{7}$$

From (6) and from (7) there follows

$$r(B\cup\{a_1,a_2,x\})=r(B\cup\{x\}).$$

A continuation of this procedure yields in the n-th step

$$r(B\cup A\cup\{x\})=r(B\cup\{x\}). \tag{8}$$

Finally from $r(A)=r(A\cup\{x\})$ we get on the basis of Lemma 2

$$r(A\cup B)=r(A\cup B\cup\{x\}) \tag{9}$$

and so by (5), (9) and (8)

$$r(B)=r(B\cup\{x\}),$$

i. e. $D[x,B]$ is valid. This proves (III).[6])

Making now use of the Corollary of Theorem 1, we can complete the proof of RADO's theorem.

2. Let L be an extension of the field K and let x and A be an element and a subset of L respectively. We define the relation $D[x,A]$ in the following way: $D[x,A]$ is to be valid if and only if x is algebraic over $K(A)$.

---

[6]) We remark that the two sets of axioms (I), (II), (III), (IV) and (R_1), (R_2), (R_3) are in fact equivalent. Indeed, if for the relation $D[x,A]$ defined on the set M conditions (I)—(IV) hold, then let $r(A)$ denote the number of elements of some maximal independent subset of the finite set $A(\subseteq M)$. By virtue of Theorem 1 $r(A)$ is uniquely determined, and it clearly satisfies (R_1)—(R_3).

If $D[x, A]$ holds, we say that x depends algebraically on A. The algebraic independence of a set and the algebraic equivalence of two sets are defined on the basis of $D[x, A]$ as the corresponding D-concepts in § 2.

It is a well-known fact that algebraic dependence has the properties (I)—(IV). So from Theorem 1 we immediately obtain the following theorem of STEINITZ [10]:

Let L be an extension of the field K and let A and B be two subsets of L, algebraically independent and equivalent (over K). Then A and B have the same cardinal number.

3. We call an element x of the group G a distinguished element, if it generates a minimal normal subgroup in G. Let us consider the set S of all distinguished elements of G, and let us define on this set the relation $D[x, A]$ in the following manner: $D[x, A]$ is to be valid if and only if $x(\in S)$ is an element of the normal subgroup generated by $A(\subseteq S)$. It is evident that (I), (III) and (IV) are fulfilled. The validity of (II) can also be shown without difficulty. Let $D[x, A]$ and $\overline{D}[x, A \setminus \{a\}]$, $a \in A$ hold. Then a relation of the form $x = bc$ holds, where c is an element, different from 1, of the normal subgroup generated by the element a, and b is an element of a normal subgroup generated by a finite subset of A not containing the element a. Hence we obtain $b^{-1}x = c(\neq 1)$, and since the normal subgroup generated by c contains, in view of the distinguishedness of a, the element a, a is in fact an element of the normal subgroup generated by $(A \setminus \{a\}) \cup \{x\}$, so that $D[a, (A \setminus \{a\}) \cup \{x\}]$. If we define independence in an analogous manner as in § 2, we can infer from Theorem 1 that two maximal independent subsets of the set of all distinguished elements of G have the same cardinal number.

In view of this fact, it is not hard to establish the following

Theorem 2. *Let G be a group which is decomposable into the direct product of simple groups. If $G = \prod_{\mu \in \Gamma} H_\mu$ and $G = \prod_{\nu \in \Delta} K_\nu$ are two such decompositions of G, then Γ and Δ have the same cardinal number.*

To complete the proof, let us take from each direct factor H_μ and K_ν exactly one element $h_\mu(\neq 1)$ and $k_\nu(\neq 1)$ respectively. Then the sets $\{h_\mu\}_{\mu \in \Gamma}$ and $\{k_\nu\}_{\nu \in \Delta}$ are maximal independent subsets of the set of distinguished elements of G, having thus equal cardinality on the basis of our above results.

In the same manner we can obtain an analogous result for the case of rings (modules) decomposable into the direct sum of simple rings (irreducible modules). For modules this result is already known (see [2], p. 62 and [3]). The theorem on modules clearly comprises also the theorem on the dimension of a vector space over a skewfield.

4. Any two maximal independent systems of elements of a torsion-free abelian group have the same cardinal number (see, for instance, [6] or [1]). However, this result does not carry over to modules with an arbitrary domain of operators. As a further application of Theorem 1 we determine the class of all rings R which are such that the result just mentioned holds for every torsion-free R-module.[7])

This problem can be considered in two different ways. Module theory is often restricted to the case where R has a unit element which acts as identity operator; then we talk about unitary R-modules. The order of an element g of a unitary R-module G is the set of all r ($\in R$) such that $rg=0$. G is torsion-free if all its nonzero elements are of order zero. The element g is dependent on the subset A of G if, for some r ($\in R$), $rg \neq 0$ and rg belongs to the submodule generated by A; independence is defined accordingly, as in § 2.[8]) — On the other hand, in a general approach to module theory no restrictions are necessary: every R-module is considered as a unitary R^*-module in a natural way, and order, dependence, etc., are then defined in terms of R^*.[9]) Note that most statements on a module depend on whether it is considered as a unitary R-module (if it can be considered as such) or just as an R-module (in the general sense).

In both cases the solution of the problem leads essentially to the class of regular rings in the sense of O. Ore [7]. There a ring R is called *regular* if it has no zero divisors and if, for every two nonzero elements a, b of R, the equation $xa+yb=0$ has a nontrivial solution in R. We shall also use the following equivalent definition: R is regular if it has no zero divisors and if any two nonzero left ideals of R have nonzero intersection.

---

[7]) An R-module G is an (additive) abelian group with the (associative) ring R as a left operator domain.

[8]) It follows immediately that an arbitrary set of nonzero elements $g_1, g_2, \ldots$ of G is independent if and only if for every finite subset of this set a relation

$$r_1 g_{i_1} + \cdots + r_n g_{i_n} = 0 \qquad (r_j \in R;\ j = 1, \ldots, n)$$

always implies

$$r_1 g_{i_1} = \cdots = r_n g_{i_n} = 0.$$

If G is torsion-free, then the latter equalities imply $r_1 = \ldots = r_n = 0$.

[9]) See [4]. In particular, R^* is the Dorroh-extension of R by a formal unit element. A set of nonzero elements $g_1, g_2, \ldots$ of G is independent in this sense if for every finite subset of this set a relation

$$\langle r_1, n_1 \rangle g_{i_1} + \cdots + \langle r_k, n_k \rangle g_{i_k} = 0$$

always implies

$$\langle r_1, n_1 \rangle g_{i_1} = \cdots = \langle r_k, n_k \rangle g_{i_k} = 0.$$

If G is torsion-free, then the latter equalities imply $\langle r_1, n_1 \rangle = \ldots = \langle r_k, n_k \rangle = \langle 0, 0 \rangle$. For the notation $\langle r_j, n_j \rangle$ see also [4].

Theorem 3. *Let R be a ring with unit element* 1. *In order that*

(A) *any two maximal independent systems of elements of any torsion-free unitary R-module have the same cardinal number, it is necessary and sufficient that one of the following conditions hold:*

(a) *R has zero divisors;*

(b) *R is regular.*

Theorem 4. *Let R be any ring. In order that*

(B) *any two maximal independent systems of elements of any torsion-free R-module have the same cardinal number, it is necessary and sufficient that one of the following conditions hold:*

(a) *R has zero divisors;*

(a′) *R has nonzero elements of finite additive order;*

(a″) *R contains a nontrivial subring isomorphic to a subring of the rational integers;*

(b) *R is regular.*

Proof of Theorem 3. Suppose first that (A) holds and that R has no divisors of zero. Then R considered as a unitary R-module is torsion-free, and has 1 as a maximal independent system of elements. By virtue of (A) any two nonzero elements a, b of R are not independent, and consequently the equation $xa+yb=0$ admits a nontrivial solution. So R is regular.

Conversely, let (a) or (b) be fulfilled. If R has divisors of zero, then there exist no torsion-free unitary R-modules, and so (A) holds. Let now the ring R be regular. By virtue of Theorem 1, in order to establish the validity of (A), it will be sufficient to show that in the case of torsion-free unitary modules the dependence of an element x on a set A, which from now on we shall denote by $D[x, A]$, has the properties (I)—(IV).

(I), (II) and (IV) are clearly valid. Let G be a torsion-free unitary R-module and let $D[g, U]$, $D[U, V]$ be fulfilled. We show that $D[g, V]$ is also valid. According to (IV) $D[g, U]$ means that, for a suitable finite subset $u_1, \dots, u_k$ of U, a relation of the form

$$r_0 g = r_1 u_1 + \cdots + r_k u_k \tag{10}$$

holds. In view of $D[U, V]$ and (IV) for suitably chosen elements v_{ij} of V we likewise have the equalities

$$\left\{\begin{array}{ll} r_{10} u_1 = r_{11} v_{11} + \cdots + r_{1m_1} v_{1m_1} & (r_{10} \neq 0) \\ \quad\vdots & \\ r_{k0} u_k = r_{k1} v_{k1} + \cdots + r_{km_k} v_{km_k} & (r_{k0} \neq 0). \end{array}\right. \tag{11}$$

We may suppose that in the equalities (10) and (11) all elements occurring are different from zero. So, by the regularity of R, there exist elements s_α $(\neq 0)$ and s'_α $(\neq 0)$ $(\alpha = 1, 2, \dots, k)$ of R, for which

$$(12)\qquad \begin{cases} s_1 r_1 u_1 = s'_1 r_{10} u_1 \\ s_2 s_1 r_2 u_2 = s'_2 r_{20} u_2 \\ \vdots \\ s_k \dots s_2 s_1 r_k u_k = s'_k r_{k0} u_k. \end{cases}$$

Let us now multiply (10) (from the left) by s_1, and the first equation of (11) again from the left by s'_1; by virtue of (12) the element $s_1 r_1 u_1$ can be replaced in the multiplied equation (10) by a linear combination (over R) of the elements v_{ij}. Multiplying the expression so obtained by s_2, and the second equation (11) by s'_2, we effect a further replacement, again on the basis of (12). By a continuation of this process we are able to show finally that the element

$$s_k \dots s_2 s_1 r_0 g \ (\neq 0)$$

is contained in the submodule of G generated by the set V, giving $D[g, V]$. This completes the proof of Theorem 3.

Proof of Theorem 4. Let us assume first that (B) holds for R; then (A) holds for R^* and so, according to Theorem 3, either (a) or (b) holds for R^*. If R^* has zero divisors then there can be no torsion-free R-modules. In particular, R itself considered as an R-module is not torsion-free: there is an r $(\in R, r \neq 0)$ whose order is a nonzero subring S of R^*. If $S \cap R \neq 0$ then (a) holds for R. If S contains an element of the form $\langle 0, n \rangle$ then R satisfies (a′). If neither of these happens, then there is a one-to-one correspondence between the first and second components of the elements of S, and this is an isomorphism of the kind required for (a″). On the other hand, if R^* is regular then from the second definition of regularity one sees at once that (b) is satisfied by R.

Conversely, if (a) or (a′) holds then R^* evidently has zero divisors; and if r $(\neq 0)$ corresponds to n in an isomorphism provided by (a″), then $\langle r, -n \rangle \langle r, 0 \rangle = 0$ shows the same. So in these cases there are no torsion-free R-modules. If none of (a), (a′), (a″) holds, then, by what has been said above, R^* cannot have zero divisors. It remains to be shown that in this case (b) implies the regularity of R^*. This will follow if we prove that every nonzero left ideal L of R^* has nonzero intersection with R. But since $rl \in R \cap L$ for every $r \in R$, $l \in L$, it is certainly true (except in the obvious case of $R = 0$). So the application of Theorem 3 completes the proof.

References

[1] L. Fuchs, *Abelian groups* (Budapest, 1958).
[2] N. Jacobson, *Structure of rings* (Providence, 1956).
[3] A. Kertész, Beiträge zur Theorie der Operatormoduln, *Acta Math. Acad. Sci. Hung.*, 8 (1957), 235—257.
[4] A. Kertész, A remark on the general theory of modules, *Publ. Math. Debrecen,* 6 (1959), 86—89.
[5] A. Kertész, Simple proof of a fundamental theorem of field theory, *Amer. Math. Monthly,* 66 (1959), 804.
[6] А. Г. Курош, Теория групп (Москва, 1953).
[7] O. Ore, Linear equations in non-commutative fields, *Ann. of Math.*, 32 (1931), 463—477.
[8] G. Pickert, *Einführung in die Höhere Algebra* (Göttingen, 1951).
[9] R. Rado, Axiomatic treatment of rank in infinite sets, *Canadian Journal of Math.*, 1 (1949), 337—343.
[10] E. Steinitz, *Algebraische Theorie der Körper* (Berlin, 1930).
[11] B. L. van der Waerden, *Moderne Algebra.* I (Berlin—Göttingen—Heidelberg, 1950).
[12] H. Whitney, On the abstract properties of linear dependence, *American Journal of Math.*, 57 (1935), 509—533.

(Received February 29, 1960)